NISTIR 5155

Guide to Voice Privacy Equipment for Law Enforcement Radio Communications Systems

P. Michael Fulcomer

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Electronics and Electrical Engineering Laboratory
Electricity Division
Gaithersburg, MD 20899

Prepared for
National Institute of Justice
Office of Justice Programs
U.S. Department of Justice
Washington, DC 20531

NIST

ABOUT THE TECHNOLOGY ASSESSMENT PROGRAM

The Technology Assessment Program is sponsored by the Office of Development, Testing, and Dissemination of the National Institute of Justice (NIJ), U.S. Department of Justice. The program responds to the mandate of the Justice System Improvement Act of 1979, which created NIJ and directed it to encourage research and development to improve the criminal justice system and to disseminate the results to Federal, State, and local agencies.

The Technology Assessment Program is an applied research effort that determines the technological needs of justice system agencies, sets minimum performance standards for specific devices, tests commercially available equipment against those standards, and disseminates the standards and the test results to criminal justice agencies nationwide and internationally.

The program operates through:

The *Technology Assessment Program Advisory Council* (TAPAC) consisting of nationally recognized criminal justice practitioners from Federal, State, and local agencies, which assesses technological needs and sets priorities for research programs and items to be evaluated and tested.

The *Office of Law Enforcement Standards* (OLES) at the National Institute of Standards and Technology, which develops voluntary national performance standards for compliance testing to ensure that individual items of equipment are suitable for use by criminal justice agencies. The standards are based upon laboratory testing and evaluation of representative samples of each item of equipment to determine the key attributes, develop test methods, and establish minimum performance requirements for each essential attribute. In addition to the highly technical standards, OLES also produces user guides that explain in nontechnical terms the capabilities of available equipment.

The *Technology Assessment Program Information Center* (TAPIC), operated by a grantee, which supervises a national compliance testing program conducted by independent agencies. The standards developed by OLES serve as performance benchmarks against which commercial equipment is measured. The facilities, personnel, and testing capabilities of the independent laboratories are evaluated by OLES prior to testing each item of equipment, and OLES helps the Information Center staff review and analyze data. Test results are published in Consumer Product Reports designed to help justice system procurement officials make informed purchasing decisions.

Publications issued by the National Institute of Justice, including those of the Technology Assessment Program, are available from the National Criminal Justice Reference Service (NCJRS), which serves as a central information and reference source for the Nation's criminal justice community. For further information, or to register with NCJRS, write to the National Institute of Justice, National Criminal Justice Reference Service, Washington, DC 20531.

Michael J. Russell, Acting Director
National Institute of Justice

NISTIR 5155

Guide to Voice Privacy Equipment for Law Enforcement Radio Communications Systems

P. Michael Fulcomer

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Electronics and Electrical Engineering Laboratory
Electricity Division
Gaithersburg, MD 20899

Prepared for
National Institute of Justice
Office of Justice Programs
U.S. Department of Justice
Washington, DC 20531

March 1993

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Raymond G. Kammer, Acting Director

ACKNOWLEDGMENTS

This report was prepared by the Office of Law Enforcement Standards (OLES) of the National Institute of Standards and Technology (NIST), A. George Lieberman, Manager, Communications Systems, and Lawrence K. Eliason, Director of OLES. The research resulting in this report was part of the National Institute of Justice Technology Assessment Program, David G. Boyd, Director, Science and Technology. The technical effort to develop this report was conducted under Interagency Agreement LEAA-J-IAA-021-3, Project No. 8901.

FOREWORD

The Office of Law Enforcement Standards (OLES) of the National Institute of Standards and Technology (NIST) furnishes technical support to the National Institute of Justice (NIJ) program to strengthen law enforcement and criminal justice in the United States. OLES's function is to conduct research that will assist law enforcement and criminal justice agencies in the selection and procurement of quality equipment.

OLES is: 1) Subjecting existing equipment to laboratory testing and evaluation and 2) conducting research leading to the development of several series of documents, including national voluntary equipment standards, user guides, and technical reports.

This document covers research on law enforcement equipment conducted by OLES under the sponsorship of NIJ. Additional reports as well as other documents are being issued under the OLES program in the areas of protective equipment, communications equipment, security systems, weapons, emergency equipment, investigative aids, vehicles, and clothing.

Technical comments and suggestions concerning this report are invited from all interested parties. They may be addressed to the Office of Law Enforcement Standards, National Institute of Standards and Technology, Gaithersburg, MD 20899.

Lawrence K. Eliason, Director
Office of Law Enforcement Standards

TABLE OF CONTENTS

COMMONLY USED SYMBOLS AND ABBREVIATIONS

A	ampere	H	henry	nm	nanometer
ac	alternating current	h	hour	No.	number
AM	amplitude modulation	hf	high frequency	o.d.	outside diameter
cd	candela	Hz	hertz (c/s)	Ω	ohm
cm	centimeter	i.d.	inside diameter	p.	page
CP	chemically pure	in	inch	Pa	pascal
c/s	cycle per second	ir	infrared	pe	probable error
d	day	J	joule	pp.	pages
dB	decibel	L	lambert	ppm	part per million
dc	direct current	L	liter	qt	quart
°C	degree Celsius	lb	pound	rad	radian
°F	degree Fahrenheit	lbf	pound-force	rf	radio frequency
diam	diameter	lbf·in	pound-force inch	rh	relative humidity
emf	electromotive force	lm	lumen	s	second
eq	equation	ln	logarithm (natural)	SD	standard deviation
F	farad	log	logarithm (common)	sec.	section
fc	footcandle	*M*	molar	SWR	standing wave ratio
fig.	figure	m	meter	uhf	ultrahigh frequency
FM	frequency modulation	min	minute	uv	ultraviolet
ft	foot	mm	millimeter	V	volt
ft/s	foot per second	mph	mile per hour	vhf	very high frequency
g	acceleration	m/s	meter per second	W	watt
g	gram	N	newton	λ	wavelength
gr	grain	N·m	newton meter	wt	weight

area = unit^2 (e.g., ft^2, in^2, etc.); volume = unit^3 (e.g., ft^3, m^3, etc.)

PREFIXES

d	deci (10^{-1})	da	deka (10)
c	centi (10^{-2})	h	hecto (10^2)
m	milli (10^{-3})	k	kilo (10^3)
μ	micro (10^{-6})	M	mega (10^6)
n	nano (10^{-9})	G	giga (10^9)
p	pico (10^{-12})	T	tera (10^{12})

COMMON CONVERSIONS

(See ASTM E380)

ft/s×0.3048000 = m/s	lb×0.4535924 = kg
ft×0.3048 = m	lbf×4.448222 = N
ft·lbf×1.355818 = J	lbf/ft×14.59390 = N/m
gr×0.06479891 = g	lbf·in×0.1129848 = N·m
in×2.54 = cm	lbf/in^2×6894.757 = Pa
kWh×3 600 000 = J	mph×1.609344 = km/h
	qt×0.9463529 = L

Temperature: $(T_{°F}-32)\times 5/9 = T_{°C}$

Temperature: $(T_{°C}\times 9/5)+32 = T_{°F}$

GUIDE TO VOICE PRIVACY EQUIPMENT FOR LAW ENFORCEMENT RADIO COMMUNICATIONS SYSTEMS

P. Michael Fulcomer*
Electronics and Electrical Engineering Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

In many parts of the country, secure voice communication has almost become a necessity if law enforcement agencies are to successfully compete against the criminal. Voice privacy is the term used to denote the ability of a communication system to conceal the content of voice messages from unauthorized persons. It can, in some cases, be added to an existing communications system, or an entirely new system with voice privacy included may be purchased. There are various methods utilized to achieve voice privacy, with level of security, voice quality, effect on transmission range, complexity of operation and cost being some of the variables. The various methods can be separated into two major categories — analog and digital. The term "scrambler" is often used for analog devices, whereas "encryption" is used for the digital devices. This guide is intended to provide state and local law enforcement agencies with guidance in the selection and use of voice scrambling and encryption devices for use with personal/mobile transceivers. The information in it comes from both users and manufacturers, and from organizations that are working towards a new digital transmission standard.

Key words: analog scrambler; communications; digital encryption; encryption; land mobile radio; law enforcement; scrambler; secure voice communications; voice privacy

1. INTRODUCTION

In many parts of the country, secure voice communication has almost become a necessity if law enforcement agencies are to successfully compete against the criminal. Narcotics and vice are but two areas where successful interdiction requires that the perpetrators not be able to listen in on plans to disrupt their operation. Even ordinary citizens, listening in on relatively inexpensive police radio scanners can rush to the scene of a crime, accident or civil disturbance, and unintentionally disrupt police activities.

---

*Electricity Division.

Voice privacy is the term used to denote the ability of a communication system to conceal the content of voice messages from unauthorized persons. It should be noted that the advent of mobile digital data terminals has, for those agencies that possess them, eliminated the need for voice communications in certain situations. These situations ordinarily do not include catching criminals in the act, however, where instant command and response on portable transceivers away from the police vehicle is often required.

Various methods are utilized to achieve voice privacy, with level of security, voice quality, effect on transmission range, complexity of operation and cost being some of the variables. The various methods can be separated into two major categories — analog and digital. The term "scrambler" is often used for analog devices, whereas "encryption" is used for the digital devices. When the previous edition of this guide was printed in 1976, digital encryption devices were rare and not cost effective except for government and military operations that required the highest level of security available. Since that time, improvements have been made in both categories so that both analog and digital types are presently used by law enforcement agencies. The devices in the latter category generally provide the highest levels of security, but sometimes at the expense of the other variables mentioned above.

This guide is intended to provide state and local law enforcement agencies[1] with guidance in the selection and use of voice scrambling and encryption devices for use with personal/mobile transceivers. Sources of information for the guide include users and manufacturers of voice privacy equipment, and organizations that are working towards a new digital transmission standard that may someday determine the most effective way to provide voice privacy.

In some cases, voice privacy can be added to an existing communications system. It is also possible to purchase an entirely new system with voice privacy included. In either case the law enforcement agency will need to:

(a) identify its requirements,
(b) determine what equipment is available that can satisfy those requirements,
(c) obtain and evaluate proposals from suitable suppliers,
(d) award the contract,
(e) evaluate the performance of installed equipment and rectify any faults.

Initial decisions may have to be modified and compromises made in order to match agency needs and funding to the features and cost of available voice privacy systems.

This guide does not specifically address the security of either cellular or land line telephone conversations, but the privacy concerns are nearly the same as they are for

[1]Government law enforcement agencies and the military are required to use special digital encryption systems, designated as Type I, for protection of classified information. These systems are generally not available for state and local law enforcement use.

personal/mobile transceivers. Separate systems are available that provide security for telephone communications.

2. GENERAL CONSIDERATIONS

2.1 General Approaches to Voice Privacy

There are two general approaches to achieving voice privacy — analog and digital. Analog devices, by convention called scramblers, systematically modify the continuously varying analog voice signal. This scrambled signal is then used to modulate a normal FM transmitter. The transmitted signal is received, demodulated and descrambled in the receiver. It should be noted that for added security the "systematic modification" mentioned above is usually controlled by a continuously changing digitally generated code. The device is categorized as analog because it is an analog signal that is scrambled and transmitted.

A digital device first converts the analog voice signal to digital and then scrambles or encrypts (the latter being the term normally used for digital) the resulting signal. The encrypted signal modulates the transmitter using some form of digital modulation. The receiver demodulates and decrypts the signal before converting it back to analog.

Analog scramblers can be subdivided further into (1) those that scramble in the frequency domain, i.e., rearranging the frequency components of the speech signal to produce unintelligible sounds, (2) those that scramble in the time domain, i.e., dividing the speech signal into short time segments and rearranging those segments before transmission, and (3) those that combine the two methods. All other things being equal, the time domain scrambler will have a higher level of security but at the cost of a possibly significant delay between a speakers utterance at the transmitter and the reconstructed message output from the receiver. This delay would be particularly objectionable in the context of a duplex system, i.e., a two-way radio communication system. The time domain scramblers presently available are extremely expensive and are aimed more toward military or federal intelligence work.

Analog scramblers can also be categorized as using either (1) fixed codes, or (2) continuously changing codes. Fixed code scramblers generate the scrambled voice signal in the same manner during each transmission. This is not sufficient protection against a determined opponent — even if the code is changed daily. Scramblers that utilize a continuously changing code do so in a manner or sequence determined by a "key." An opponent is forced to use cryptanalysis in order to determine the key and eventually unscramble the message.

Digital voice privacy systems also require the use of a key or keys. Common to both analog and digital systems is the necessity for synchronization signals to accompany each transmission so that the receiver will know the precise moment to start the unscrambling

procedures. Further discussion of scrambling methods, keys and synchronization signals is contained in Section 4.

2.2 Difficulties in Providing Voice Privacy

A number of difficulties must be overcome in order for the designer to provide an effective voice privacy system. Some are related to the nature of speech, some to the particular approach taken, i.e., analog or digital, and some to the characteristics of the communications system. A brief overview will help bring these difficulties into perspective.

Speech is extremely robust and redundant in the sense that not every syllable of every word need be comprehended in order to understand a verbal communication. The human perception is so great that speech can be grossly distorted by various forms of mutilation and still be intelligible, if it remains in analog form. This is one of the difficulties that analog voice privacy systems must overcome and some do it much better than others.

Speech converted to digital signals is not intelligible under any circumstances, but digital voice privacy systems have difficulties in other areas. One of these difficulties is the inability of some systems to achieve the same range of transmission in the encrypted mode as in the clear voice mode. Another is the constraint imposed by available bandwidth. A third is in fringe area reception, i.e., since analog voice transmission is robust and redundant, analog systems can have some advantage over digital in fringe area reception. Digital systems use error correcting codes and/or other techniques to counteract their disadvantage in this area, but this can require additional bandwidth.

Another constraint is imposed by the synchronization signals that are required for secure voice transmission by either analog or digital methods. These signals can be lost in areas where normal reception is poor or problematical. Such loss can make recovery of the secure voice signal in those areas difficult or impossible for either analog or digital systems.

Constraints on voice privacy can be imposed by the police communications system itself. The communications system may include telephone lines, repeaters, voting receivers, microwave relay links, and multiplexers to mention a few. Some of these devices could prevent correct transmission of the scrambled or encrypted signal unless they are modified in some way. Any fault or weak point in a communications system is likely to cause more serious degradation to the signal when voice privacy is introduced. As an example, telephone circuits and police radio bands require a nominal 3000 Hz audio bandwidth for voice communications. The actual bandwidth may be somewhat less than this, however, and the amplitude vs. frequency plot may have significant variation within the passband. While these limitations do not significantly affect normal unscrambled voice communications, they do impose serious constraints on a voice privacy system — particularly on digital systems and those analog systems that scramble by rearranging frequency components of the voice signal.

The major limitation to the use of digital encryptions in the past has been the lack of sufficient bandwidth. A simplified explanation for this is that (1) the more bits used in the analog to digital conversion for a given segment of speech, the better will be the intelligibility of the recovered analog signal after conversion back from digital in the receiver, and (2) the transmissions of more bits per unit of time requires additional bandwidth. Important advances have recently been made in analog to digital conversion technology however, so that now the conversion process requires fewer bits to achieve the same level of intelligibility. The bandwidth requirement for digital transmission and encryption has therefore been reduced to where digital is a viable alternative to analog.

2.3 Tradeoffs Involved

The addition of voice privacy to a communication system can reduce both voice quality (including the ability to recognize speakers) and transmission range, and increase the cost and complexity of the communications equipment. In the past, the effects on voice quality and range have been somewhat more pronounced with digital encryption. Many of the present day systems however, both analog and digital, have been improved to the point where effects on voice quality and range are hardly noticeable. Complexity and cost continue to be issues however, and both increase with the level of security desired. Increased complexity raises the possibility of more failures in the field and increased cost is always an issue, particularly when public funds are involved.

The level of security required from a voice privacy system depends upon the application. Most police departments only require a level of security sufficient to prevent a potential eavesdropper, even with fairly sophisticated skills and equipment, from decoding voice communications until the operation with which the communications are concerned is over. This could mean a matter of hours or days, depending upon the operation. Some of the more sophisticated digital systems presently available would theoretically require an eavesdropper to spend months or even years before a message could be decoded.

3. IDENTIFY REQUIREMENTS

Factors that purchasers of a voice privacy system should consider include: (1) trade-off between security level, complexity and cost (see sec. 2.3), (2) the characteristics of the communications system with which voice privacy will be used — perhaps an upgrade of the system is necessary and can be accomplished along with the addition of voice privacy, (3) environmental conditions in which the system will be used — temperature, humidity, etc..., (4) code security — what happens if a unit is lost or stolen and how are codes generated and entered into the transceivers, (5) useful battery life for portable units, (6) special requirements, such as clear voice override or multiple codes loaded into each transceiver, and (7) support and maintenance requirements.

3.1 Security Level

The security level required is determined mainly by the type of opponents from whom the conversations must be kept secret. Is the opponent likely to mount a serious attack on the system, and if he does, how capable or successful is he likely to be? What are the consequences if he succeeds? A system needed only to foil burglaries in progress or to keep the general public or special interest groups, such as tow-truck operators, ambulance services and news media people from disrupting police operations will not require as high a security level as one used to plan or monitor raids on illegal narcotic operations or to provide protection of high officials from possible terrorist attacks. A burglar will probably not have the sophisticated skills and equipment necessary to seriously attack a voice privacy system. The same is not true for a wealthy and well organized crime syndicate. If the sophisticated criminal can avoid apprehension by knowing the locations and movements of the police, he may be willing to invest a considerable amount to protect his operations. Also, instructions to a police officer to proceed to a specific location and arrest an offender need be secure only until he gets there, whereas planning for a major drug bust may require that communications be secure for months. The agency's job is to evaluate the threat as realistically as possible.

A patrol officer would not need a voice privacy system with the same level of security as would a vice or narcotics officer. However, once a department decides to go the route of voice privacy, everyone should use the same system. This prevents possible confusion and/or lack of communication if more than one system is used. Not every officer need be equipped with the secure radios in the beginning, but there is an advantage to eventually encoding all the transmissions. Once that is accomplished, the timing and the number of coded transmissions (even though they are not decoded) can no longer give evidence that an important operation is about to begin.

The level of security should match the highest level required by the situations normally encountered by the law enforcement agency. Unusual situations, such as protecting a head of state, that may require higher levels of security are normally done in conjunction with a federal law enforcement agency. Their communications system could probably be used in these special situations. If cooperation with federal agencies is commonplace, however, it would obviously be advantageous to have a system interoperable with theirs.

3.2 Communication System Requirements

After an organization determines it has a need for voice privacy and the security level established, the organization must decide whether to retrofit it into the present communication system or purchase a new one. Retrofitting is normally less expensive, but even when possible may not be the best solution if the original system is dated. Most analog voice privacy systems can be retrofitted. The addition of digital voice privacy requires that the communication system be capable of digitally coded transmission. Without that

capability in place, addition of digital voice privacy is not possible without either a partial or a complete revamping of the communications system.

If a retrofit is desired, the law enforcement agency can specify that "the voice privacy system must perform satisfactorily when used in the communications system as described" and then proceed with that description. Even if the described security cannot be obtained without a partial or complete replacement of the present communications system, the description is necessary to help match what is already there to what is needed. Important items that should be noted in the description are:

- locations of all base stations, repeaters, and satellite voting receivers
- locations of all telephone links and their frequency response characteristics
- identification of geographical areas of weak signal or high noise level
- identification of signals used to control repeaters, satellite receivers or other equipment
- identification of types and models of communications equipment in use
- identification of special features such as automatic number identification (ANI), continuous tone-controlled squelch (CTCSS), status reporting, etc. with which the voice privacy system must be compatible.

Repeaters are often controlled by signals in the audio frequency range. This can result in a situation where the control signal confuses the scrambling process or the scrambling process confuses the control signal, or both. Voting receivers may introduce abrupt phase changes because of variations in the signal path length via telephone lines. Also, the poor frequency response of some telephone links may adversely affect the scrambled signal. If so, the lines will need to be equalized to extend and flatten the response.

3.3 Environmental and Operational Considerations

In addition to performance requirements, prospective voice privacy system users need to consider a number of other factors that could influence their choice of equipment. These relate to the environment in which the system will be used, the human/system interface and other operational considerations.

Will the voice privacy system stand up to the extremes of heat and cold to which it may be exposed in mobile and portable transceivers? Does it add so much bulk or weight as to make portable operation difficult? Does it reduce battery life for portable transceivers significantly? Is it rugged enough to stand up to the rough treatment that portable transceivers sometimes receive?

Is the voice privacy system simple to operate? It is pointless to choose equipment that offers a high level of security but is too complex to be operated by nontechnical police officers, or where voice security can be compromised by incorrect operation. For example, many communication systems must be able to operate in both the clear or coded modes because not all radios in the system have coding capability. In this case, there is the potential danger that an operator might mistakenly transmit an important message in the clear when the message should have been scrambled. Switching the transmitter to clear mode should require a positive action by the operator. The receiver should have the capability of clear voice override, i.e., the receiver can detect whether a communication is clear or scrambled and then automatically switch to the correct mode. The operator should have a readily discernable means of determining whether an incoming message is clear or coded so that he or she can respond in the same mode.

Is multiple keycode capability, i.e., where more than one keycode can be loaded into each transceiver, required for the intended use of the voice privacy system? For example, in a super secret operation, a narcotics branch may wish to keep communications between its agents separately secure from those that go out to the rest of the department. Or it may be advantageous to keep communications between police and fire departments or between police and detectives separately secure. Multiple keycode capability allows different groupings to be arranged, or as discussed later, allows instant changing of the code should the system be compromised in some way.

Does a coded message remain scrambled all the way through the transmission and reception path, or does it have to be converted back to clear voice for repeaters, telephone interconnects, etc.? The location of any clear voice segment, even if confined to a remote repeater station would require additional physical security to prevent interception of the message at that point.

The following are other questions that the prospective purchaser may wish to ask. How easily can the device be maintained and repaired? Can a defective scrambler be replaced without readjusting the transceiver or the replacement scrambler? If the scrambler portion fails, can the transceiver continue to be used in the clear?

3.4 Code Security and Key Management

Protection of the scrambler code itself is a major concern. Will the voice privacy system be threatened if a transceiver is lost, stolen, or tampered with? Keys (the series of digits that determines the code sequence) must be protected from unauthorized persons and be easily changed if compromised. Some of the more sophisticated voice privacy systems have the capability whereby specific transceivers can be disabled remotely. If a transceiver is stolen, it can be disabled so that the thief cannot listen in on secure conversations. Some systems also have the capability whereby a stolen transceiver can "listen" to what is being said in its vicinity and transmit this information to other transceivers in the system. Other, even more elaborate systems, allow rekeying of individual units over the air. Since security

of the scrambler code and key management itself are both improved, over-the-air-rekeying (OTAR) is a very desirable feature. In the absence of OTAR, a desirable feature is the ability to store more than one key in each transceiver. If the system is compromised by a stolen radio or some other event, each operator can be instructed to shift to a backup key by a series of maneuvers known only to those authorized to use the transceivers, e.g., a series of numbers entered into the transceiver keypad.

3.5 Support Requirements

Support is usually required in the areas of installation, documentation, training, and maintenance. This support may be provided by the supplier, the law enforcement agency, an independent organization, or some combination of these three. Installation and documentation are normally the responsibility of the supplier or his distributor. Larger law enforcement agencies may eventually be able to assume responsibility for training and maintenance, but the supplier or his agent should be available as backup.

To avoid misunderstandings, system support required from the supplier should be clearly specified in the final contract. If someone other than the supplier is to install or maintain the equipment, provisions must be made to assure that those responsible are "cleared" for security purposes and that they receive adequate documentation and training.

4. DETERMINE EQUIPMENT AVAILABLE

The two general approaches to voice privacy, analog and digital, were described earlier in Section 2.1. To review briefly, digital encryption devices tend to offer greater security, but usually at the cost of higher price and greater complexity. The audio quality and range of transmission of digital devices can also suffer in comparison to analog type scramblers but recent developments have produced significant improvements in both areas. Analog systems can provide a level of security which is sufficient for many law enforcement application. Also, an analog system can often be added to an operating communications system without extensive modifications.

Digital voice quality is dependent, in part, on an effective means of converting the analog speech into a digital signal. In the past, the best analog to digital conversion techniques required a high bit rate (32 to 64 kb/s), and therefore a bandwidth which exceeded that available to law enforcement communication systems. More advanced analog to digital conversion techniques can produce nearly the same voice quality at lower bit rates, but until the mid 1980's these techniques were not cost effective. In these methods, the number of bits required is reduced in exchange for an increase in complexity of the analog to digital conversion technique. These more elaborate techniques look at the speech signal more carefully, reduce the redundancies in the speech signal more effectively, and use the available bits to code the nonredundant parts in a more efficient manner.

There have also been advances in analog technology during the past several years, some of them proprietary to specific manufacturers. In general, the level of security for a given cost has increased for analog voice privacy systems.

4.1 Analog Scramblers

As discussed in Section 2.1, analog scramblers can be divided into three major categories: (1) those that rearrange frequency components of the speech signal, (2) those that divide the speech signal into short time segments and then rearrange those segments and (3) those that combine the first two methods. Each category can be further subdivided into those using a fixed code, i.e., the same code is used for each transmission, and those using a continuously changing code. Scramblers that utilize the latter do so in a manner or sequence determined by the "key." A key is also used with digital encryption systems. This is discussed in more detail in Section 4.4.

The majority of analog scramblers presently available for law enforcement use fall into category (1). These include various forms of inversion and bandsplitting. Those with fixed codes generally provide only a minimum level of security and, as such, are not suitable for operations such as narcotics, vice, etc. Devices in categories (2) or (3) can have an advantage in security, but often at a great increase in price and complexity. There is also an inherent delay associated with time element scramblers that may prevent their use in duplex communication systems.

4.1.1 *Frequency Scrambling*

4.1.1.1 Inversion

Frequency inversion voice privacy systems have been available for many years, but by themselves offer a relatively low level of security. The principle involved, however, can be augmented or combined with other forms of scrambling to provide increased levels of security. With an inverter, each frequency component of the voice signal is shifted to a new frequency. The new frequency is the difference between the original frequency and a reference frequency. For example, if the reference frequency is 3300 Hz, a frequency component of 300 Hz would be converted to 3000 Hz and a frequency component of 3000 Hz would be converted to 300 Hz, i.e., the components would be inverted. This is illustrated in figure 1 for the frequencies in the nominal 300 to 3000 Hz voice band.

Inverters using a single reference frequency are fixed-code inverters and as such offer a very low level of security. Inverted speech of this type can be unscrambled by relatively inexpensive equipment and with practice can be understood by some people even without unscrambling. These devices are generally not suitable for law enforcement work except to provide privacy from casual eavesdroppers. Somewhat better are "tunable fixed code inverters" where a new reference frequency can be easily selected.

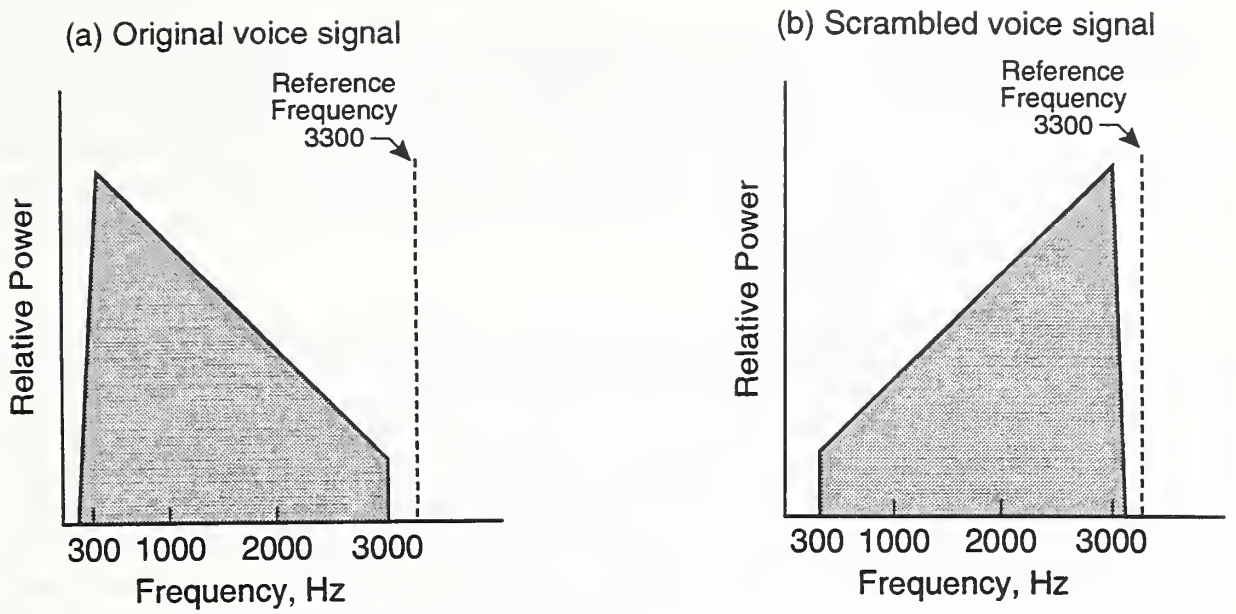

Figure 1. Scrambling by inversion.

Inverters in which the reference frequency is continually changed according to some predetermined code are known as frequency-hopping inverters[2] or, if an additional refinement is added, as band shift (or split band) inverters. Both types offer increased levels of security over that provided by fixed code inversion and are suitable for many types of law enforcement work.

Even though security is increased, the frequency-hopping inverter has a problem in that part of the audio signal is lost once the reference frequency is shifted away from the 3300 Hz given in the example. For example, if the reference frequency is shifted to 3600 Hz, a speech frequency component of 300 Hz (lower edge of the voice band) is converted to 3300 Hz and a component of 3000 Hz (upper edge of the voice band) is converted to 600 Hz. In effect, the audio passband has been shifted by an amount equal to the change in reference frequency, in addition to being inverted. Some original speech frequencies, in this case those below 600 Hz, are converted to frequencies which are above the 3000 Hz upper edge of the audio passband and, as such, are lost. This loss will not have significant effect on voice quality if it is limited to 300 or 400 Hz at either edge of the voice band but it does serve to limit the number of choices for the reference frequency and hence the security enhancing effectiveness of the frequency-hopping inverter.

[2]Some manufacturers refer to these as rolling code scramblers. The starting point and the time spent at each frequency can also be varied to further increase security.

Another factor to be considered is that small jumps in reference frequency do not provide as much security as large jumps. With small changes, an opponent could set his decoder reference frequency at some mid-point, leave it there and still be able to decode enough to make the conversation understandable. This means that some of the possible reference frequency sequences that form the code are not as effective as others, i.e., the number of possible sequences or codes listed by the manufacturer is not necessarily indicative of the security level achieved.

To avoid losing significant portions of the speech signal with larger changes in the reference frequency, the bandshift or split-band inverter shifts the lost portion to the unused opposite side of the band. For example, in the previous illustration, the original frequencies below 600 Hz that would have been converted to frequencies above 3000 Hz and lost are instead reconverted and inverted to frequencies between 300 and 600 Hz (i.e., 600 Hz becomes 300 Hz and 300 Hz becomes 600 Hz with 600 Hz being known as the "split-point"). Implementation of this scheme requires the coordination of two reference frequencies, the "high band" one which is approximately 3000 Hz above the split point and the "low band" one which is approximately 300 Hz above the split point. It also requires the use of special filters to avoid problem-causing overlaps around the split point. Even with these filters however, some loss of voice frequencies can occur. For a given level of voice quality the split-band inverter does allow a greater range of choice in reference frequencies, however, and hence a higher level of security than that provided by the plain frequency-hopping inverter.

The length of time that a continuously changing code inverter remains at each of the reference frequencies in the code sequence also has an effect on security level. Obviously, security is enhanced with shorter time intervals at each frequency, but time intervals less than about 10 ms make recovery of the original voice signal more difficult, if not impossible. Discovery of a way to use extremely short time intervals and still produce good quality voice would produce a significant increase in security for inversion scramblers.

4.1.1.2 Bandsplitting

Bandsplitters, the other major category of frequency domain scramblers, divide the speech frequency band into several sub-bands (typically five) and then rearrange them relative to one another. For increased security, the bandsplitting technique is often combined with inversion so that some or all of the sub-bands are also inverted, as shown in figure 2. A fixed code bandsplitter rearranges the sub-bands in the same order at all times. These have a relatively low level of security. Bandsplitters that continually change the order offer greater security and are sometimes called "rolling-code" bandsplitters.

Bandsplitters as a class offer somewhat more security than inverters because an opponent needs more equipment to unscramble the signal. However, as is the case with inverters, some intelligence can be recovered simply by listening repeatedly to a recording

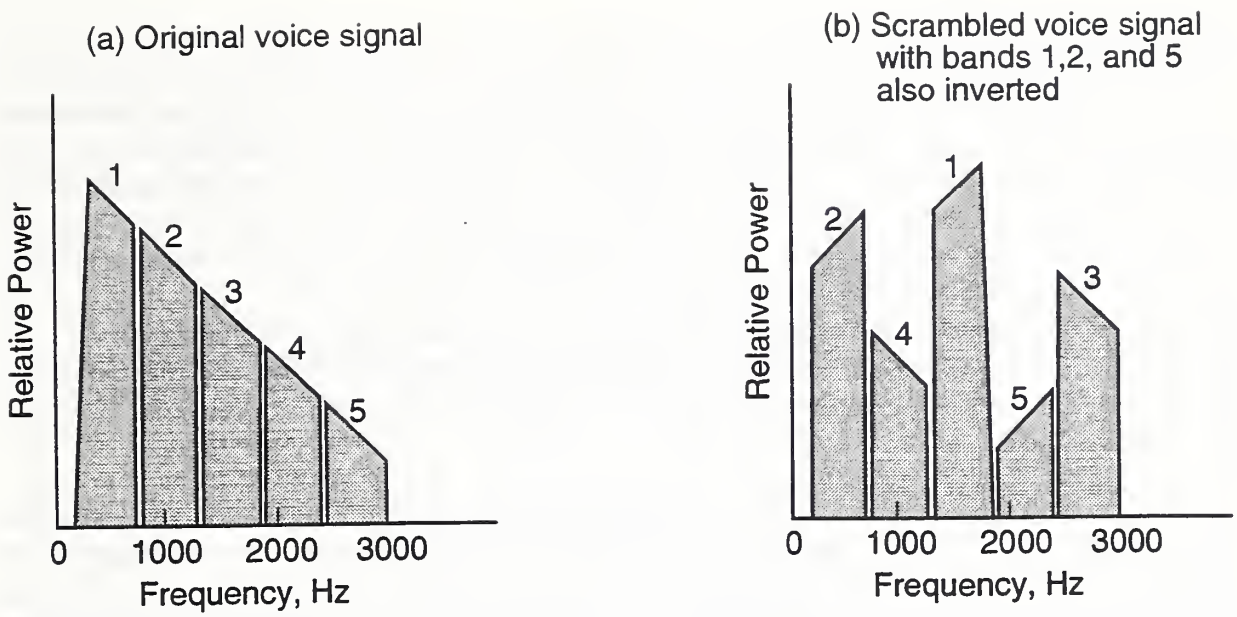

Figure 2. Scrambling by bandsplitting combined with inversion.

of the scrambled signal or by arranging only one or two of the bands back into their original positions. This is true because of the remarkable ability of the human brain to hear several conversations simultaneously and yet isolate one in particular on which to eavesdrop. If a listener is able to concentrate on one of the lower sub-bands, where much of the intelligence of the speech signal is concentrated, he may actually be able to decipher the scrambled speech by listening to it. For this reason, as was the case with inverters, not every one of all the total possible rearrangement of sub-bands can be counted as a distinctly different arrangement. Results of listening tests have suggested that (1) bands should be moved as far as possible, (2) if a band is not moved it should be inverted, and (3) bands which were adjacent originally should not remain adjacent after scrambling [1].

The security of bandsplitters can be increased by increasing the number of sub-bands, introducing a different time delay for each sub-band and/or increasing the speed at which the bands are rearranged. There is a practical limit to these enhancements however, beyond which the recovery of the original voice signal becomes very difficult. Because the filters and other components needed to separate the bands introduce extra noise and distortion into the signal, the number of sub-bands is usually limited to five or six. Some communication systems can also introduce frequency dependent delays into the transmission path — delays that make precise reconstruction of the original signal much more difficult. Purposely adding delays and/or increasing the speed of rearrangement will only aggravate this problem.

4.1.1.3 Spread Spectrum

For completeness, another technique should be mentioned. Spread spectrum transmission is not really a scrambling method, but it does provide a certain level of security and can be combined with one of the scramblers to provide a very high level of security. It is a technique whereby the transmitted signal is rapidly and randomly switched between a number of different channels. It is sometimes called frequency-hopping radio but should not be confused with the frequency-hopping invertor described earlier. In the latter, only the reference frequency for determining how the voice signal is inverted is changed — not the over-the-air transmission frequency. Without adding scrambling to the signal, security of the spread spectrum technique depends on the number of channels used and the time spent on each channel.

The system is expensive, requires a complicated synchronization scheme and obviously uses a large part of the frequency band. Because of the latter, the technique is not applicable to many situations. It should be noted, however, that in a good system, the time spent on each channel is so short that even if a number of these channels are occupied by other signals at the time, the spread spectrum transmission will still provide good communications.

4.1.2 *Time Domain Scrambling*

Scrambling in the time domain can provide greater security than scrambling in the frequency domain but with a trade-off in greater complexity and cost. Time domain scrambling can also produce a significant delay between a speaker's words at the transmitter and their reconstructed output from the receiver. The delay becomes particularly detrimental in the context of a duplex communications system[3]; but it can also be a problem for half-duplex communication[4] between officers during a coordinated action.

One popular technique for time domain scrambling is to divide the speech into time frames and then subdivide each frame into a number of segments which are rearranged within the frame. This is called time element scrambling. Unfortunately, its security is enhanced by larger frames (to increase the number of segments that can be scrambled within a frame) which also act to increase the delay in the reconstructed signal.

At the time this report was prepared, there were no time domain scramblers available for use with portable radios.[5] Because of the advances in digital encryption techniques,

---

[3]Simultaneous transmission in both directions, like an ordinary telephone.

[4]Transmission in either direction, but not simultaneously.

[5]One system is available that uses a unit housed in a briefcase. The company had no plans to introduce a smaller hand-held portable unit.

which can provide equivalent or greater security at a comparable or even lesser cost and complexity, it is unlikely that time domain scramblers will become an important factor in the nonfederal law enforcement area.

4.2 Digital Encryption Devices

4.2.1 *General*

The digital encryption voice privacy systems available for law enforcement use convert the analog voice signal that is to be protected to a digital bit stream. This bit stream or plain text is then scrambled or encrypted according to a set of rules called an algorithm before transmission as a cipher text digital signal. The receiver unscrambles or decrypts the cipher text using the algorithm in reverse and then converts the unscrambled digital or plain text back to analog voice. Until very recently, all the available digital voice privacy systems transmitted clear voice signals (not scrambled) in the analog mode, i.e., the nonsecure voice is not converted to digital at any point in the process. A more recent development is the all digital system in which both the protected and unprotected (clear voice) signals are converted to a digital bit stream. The unprotected bit stream is not subjected to encryption.

Although relatively more expensive at present, all-digital radio could become the norm rather than an exception. One of its major advantages is that noise does not accumulate over cascaded links, provided each link has sufficient bandwidth to avoid errors in the transmission of digits and/or an effective error correction scheme has been included. The newer all-digital radios use even more effective analog-to-digital conversion techniques so that both the bit rate and the bandwidth required for high quality audio can be further reduced, and the "extra" bits used for more effective error correction and/or enhanced signaling and control features. What results is a clearer voice signal in fringe areas and increased spectrum efficiency. Digital transmission also enables data to be transmitted over voice channels at a fairly high rate. Criminal records and motor vehicle license information can be accessed by mobile data terminals. Status information on a particular transceiver in the system can be sent back to the base station as digital data.

Conversion to all-digital transmission may be facilitated by a narrow band digital transmission standard for land mobile radio which is now in development[6] under the direction of the National Association of State Telecommunication Directors (NASTD) and the Associated Public-Safety Communications Officers, Inc. (APCO) with input from the Federal Government. One or more of the digital encryption algorithms necessary to achieve voice privacy, and the synchronization and key management schemes necessary for encrypted speech may also become part of this standard at some future date. When the standard is issued, any manufacturer can produce a system to the specifications of the standard and

[6]APCO Project 25. The result may be a series of standards each addressing a different aspect, rather than a single standard covering everything. See footnote 7.

systems from different manufacturers will be compatible.[7] This is usually not the situation at present. Even if the same keycode is inserted into each transceiver, a digitally encrypted voice transmission from the transceiver of one manufacturer cannot be decrypted by the transceiver of another manufacturer (see exception below). Even different systems from the same manufacturer are not necessarily interoperable.

At the time this report was prepared, there were three manufacturers of digital voice privacy systems, with Manufacturers #1 and #2 also providing the newer all-digital systems. Manufacturer #1 offers two variations of its original system and each manufacturer of the all-digital system additionally offers a choice of two encryption algorithms for both their original and all-digital systems. The system from Manufacturer #3 is interoperable with one of the original systems from Manufacturer #1.

In addition to the enhanced analog-to-digital conversion technique of its all-digital system, Manufacturer #1 also increases the number of discrete levels used in transmission of the digital signal from two to four. Increasing the number of levels allows for either (1) increasing the transmission bit rate for a given bandwidth, or (2) decreasing the bandwidth for a given transmission rate (or some combination of the two). A decrease in signal-to-noise ratio can occur, however, as the number of levels increases.

Certain radios produced by Manufacturer #1 are "interoperable" with each of the digital voice privacy systems of that manufacturer. The same is true for Manufacturer #2. This interoperability is obtained by including the necessary sections of each voice privacy system in the same radio. Reception of a different voice privacy system is not automatic — the user must manually switch between the systems.

4.2.2 *Basic Encryption Methods*

The encryption algorithm determines the process, i.e., the set of general rules, used to encrypt a digital signal, and the "key" determines the specifics. The numbers or symbols comprising the key are converted to digital, manipulated according to a portion of the algorithm rules and then combined with the plain text after it too has been manipulated by another portion of the algorithm. The combining process is determined by the procedures contained in the algorithm. The cipher text output thus depends both on the algorithm and on the key.

Since the procedures used to encrypt the plain text, i.e., the algorithm, must be implemented either in hardware or software, a determined opponent conceivably could learn what these procedures are. However, the algorithm need not be kept secret provided the key is sufficiently long and the encryption procedures sufficiently complex. In fact, security is enhanced when mere discovery of the algorithm does not compromise the voice privacy

---

[7]To enable interoperability between radio telecommunication systems of the Federal Government, a standard method for conversion of analog voice to digital (and the reverse) has already been published [2].

system. Security of the key is another matter and "key management" is one of the factors that must be addressed when judging a digital encryption system. Keys and key management are discussed in Section 4.4.

The search for a "standard" secure algorithm led to development of the Data Encryption Standard (DES) in the mid 1970's. It was originally targeted and is still used for the protection of sensitive but unclassified computer data in federal computer systems, but has since become a standard for voice encryption as well. The standard scheme ensures the interoperability of various computer systems nationwide. The same reasoning can also apply to voice communications where interoperability between different agencies may be required for the most effective law enforcement. This is particularly true for federal law enforcement agencies.

The DES consists of 16 "rounds" of operations that mix the plain text and a 56 bit key together in a prescribed manner so that there is no correlation between the resulting cipher text and either the original plain text or the key. The DES has been evaluated by several organizations and been found to be mathematically sound. It is the only algorithm approved for the protection of sensitive but unclassified data in federal computer systems. The only seriously proposed attacks involve exhaustively testing all possible keys until the correct key is found. The time and cost involved in this process are considered infeasible for the intended applications of the DES.

There are four different methods of implementing DES [3]. The methods are not interoperable. Two of these methods (cipher feedback and output feedback) are used in digital encryption systems presently available for law enforcement use. Manufacturers #1 and #3 use the cipher feedback mode while Manufacturer #2 uses the output feedback mode. Manufacturer #1 also offers another implementation of DES which they identify as the counter-addressing mode (CAM). Although this technique is not one of the four standard modes specified in 1980, it has been approved by the National Security Agency (NSA) for use in certain voice privacy systems.

Plain text is combined with the DES output to produce cipher text in each mode of operation, but in the cipher feedback mode the cipher text is fed back to the algorithm and used to determine output after the first n bits. The encryption scheme for a section of cipher text thus depends not only on the algorithm and the key, but also on the immediately preceding section of cipher text. In the output feedback mode, cipher text is not fed back to the algorithm. This encryption scheme depends only upon interaction of the key with the plain text as prescribed by the algorithm.

The advantage of the cipher feedback implementation is that it is self synchronizing. The receiver does not need a separate synchronization signal to begin decryption at the correct time. As noted in the last paragraph, the cipher feedback encryption scheme depends in part upon the immediately preceding section of cipher text, i.e., location within the stream of conversation is coded into the encryption scheme. Decryption merely reverses

the process to produce the original clear voice. With the output feedback implementation, the encryption scheme is independent of the previous cipher text. Separate synchronization signals must be sent to keep the receiver in step with the transmitter.

A disadvantage of the cipher feedback implementation is that error propagation occurs. Because the decryption of a section[8] of text depends in part upon the preceding section of cipher text, a one bit error occurring during transmission of a section of cipher text causes the following section of decrypted bits in the receiver to be totally random. Single bit errors, which can be caused by co-channel interference, intermodulation products, multipath fading, etc. are fairly common, particularly in the fringe area of reception. A single bit error is not normally a problem, however, unless it is magnified or propagated to succeeding sections of text. The practical result of bit error propagation in the cipher feedback mode of operation is loss of range in the encrypted mode over that which can be achieved in the clear mode. It can also make a workable, but noisy channel almost unusable. One way around this situation is to upgrade the communications channel by increasing the power and/or number of repeaters used.

The addition of synchronization bits, required by the output feedback implementation of DES or any other implementation that is not self synchronizing, such as CAM, has the potential advantage of no loss in range in the encrypted mode compared to that which can be achieved in the clear mode. A potential disadvantage is that the synchronization bits take away bits that would otherwise have been used to characterize the voice signal. Fewer bits can mean a decrease in voice quality, if everything else is equal. New and improved coding schemes can theoretically more than make up for the loss of some bits to the synchronization process, however.

Two present manufacturers (#1 and #2) of digital voice privacy systems also offer their own proprietary algorithm as an alternative to the DES algorithm. The proprietary algorithm could have either a smaller or larger number of total possible combinations. Even if the number is smaller, however, once one gets into millions of combinations, the reduction of security, at least for law enforcement work, is probably negligible. The DES has an advantage in that its implementation is specified by both manufacturers to conform to the requirements contained in Federal Information Processing Standard (FIPS) 140 [4]. This standard addresses physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference and compatibility (EMI/EMC), and self testing among other items. A revised and updated version, FIPS 140-1, should be issued in 1993.

Some presently available digital voice privacy systems employ bit rates which exceed those desirable for low adjacent channel interference. As noted earlier, the higher bit rates are necessary for good voice quality but they also require a greater bandwidth for

[8]A section is normally 64 bits.

transmission. Where it becomes a problem, adjacent channel interference can be reduced by increasing the spacing between channels. This, however, prevents the most efficient use of valuable spectrum space. As noted earlier in this section, advances in analog to digital conversion techniques are already leading to the development of lower bit rate systems.

For its original system, Manufacturer #1 uses continuously variable slope delta (CVSD) modulation for analog-to-digital conversion and a 12 kb/s data rate. CVSD technology is fairly mature. It increases the efficiency of each bit by coding the difference between the actual and predicted value of the analog signal — not the actual signal itself. Efficiency is further increased by using a coding scheme that adapts itself to the characteristics of the signal.

Manufacturer #2 uses sub-band coding (SBC) for analog-to-digital conversion and a 9.6 kb/s data rate. In SBC, the speech band is divided into four contiguous bands by a bank of bandpass filters. Bit efficiency is increased by assigning bits to each band based upon where they are required for best intelligibility. For normal speech, relatively more bits are assigned to the lower frequency bands.

Both manufacturers use a 9.6 kb/s data rate for their all-digital voice privacy systems, but analog-to-digital conversion and transmission modulation are different for each manufacturer. The systems are not interoperable.

The advent of the newer all-digital systems has broadened applications of digital voice privacy in the 800 MHz band (trunking radio). For the smaller agencies in particular, the use of trunking radio[9] was sometimes not desirable because it often required sharing channels with non-law enforcement agencies. (Larger agencies usually can have their own self-contained trunking system.) Now, however, the ability to program priority, i.e., to give certain operators first choice for a vacant channel, has made trunking an option even for the smaller agencies.

4.3 Synchronization

The descrambler in any voice privacy system, whether it be analog or digital, applies the scrambling procedure in reverse to recover the clear voice signal. It is obvious that the descrambling procedure must be matched perfectly in time to, i.e. in synchronization with, the incoming scrambled signal or clear voice cannot be recovered. This matching is achieved by synchronization[10] signals which are transmitted along with the scrambled signal.

---

[9]The automatic sharing of a group of communication paths among a large number of users.

[10]As previously mentioned, one method of digital encryption is self synchronizing.

There are two basic methods for sending the synchronization signals. In *initial synchronization only*, the sync information is sent at the beginning of each transmission. A clock in the receiver keeps the descrambling procedures in step with the incoming signal following the initial sync. In *continuous synchronization*, the synchronization signals are sent at regular intervals along with the scrambled signal.

Continuous synchronization has the advantage of permitting late entry, i.e., it allows an operator to hear the later portions of a message even if he was not tuned into the beginning. Continuous synchronization also allows the feature "clear voice override" to be included in the system. In this mode, manual switching of the receiver between scrambled and clear is not necessary. The receiver recognizes either the presence or absence of sync pulses (which are sent only in the scrambled mode) and sets the operation accordingly.[11] Another advantage of continuous synchronization is that poor reception of the synchronization signal does not cause loss of the entire voice message. At most, only a portion of a word may be lost.

There are two disadvantages of continuous synchronization. The first is that the sync pulses use up some of the bandwidth necessary for transmission of good quality speech, i.e., they either use all of the bandwidth for short periods of time or a portion of the bandwidth all of the time. Using the entire bandwidth for short periods of time to transmit the sync signal is more robust (less chance of losing synchronization due to a poor quality line), but results in either noise bursts or silence during the sync period. The method of application and length of the sync period determine how objectionable this may be. Using a portion of the voice bandwidth continuously for transmission of the sync signal may have less effect on speech quality, but this method usually requires that the sync pulses be transmitted at lower power. This increases the chance that synchronization will be lost.

The second disadvantage of continuous synchronization is that the same signals which allow late entry by a legitimate receiver could also enable an opponent to determine how much of a message he has missed and eventually determine the sequence. This is not as much of a problem for digital systems as analog. In the former the encryption algorithms are such that little useful information could be gained even if it were possible for an opponent to separate the synchronization signals from the digitally encrypted speech. Many analog systems get around this problem and increase security at the same time by transmitting a "time-of-day" (TOD) signal along with the synchronization.

The TOD signal, which changes at each synchronization update, is mixed with the key in the transmitter and used to select the starting point of a pseudo-random sequence generator that determines the values of time, frequency, etc. to use in the analog coding process. *Each synchronization update thus produces a different starting point and a different pseudo-random sequence of values.* The transmitted TOD is mixed with the key in the

---

[11]Clear voice override is available with initial synchronization only from at least one manufacturer but will not function for late entry decoding of scrambled messages.

receiver to initiate the same sequences at the correct time for decoding the scrambled signal. To prevent a missed TOD signal from subverting the descrambling process, the TOD signals can be designed to follow a predictable sequence — such as by using the outputs from a linear feedback shift register. Even though predictable, the sequence can be very long and the starting point chosen at random by the transmitter at each activation of the push-to-talk (PTT) switch.

Initial synchronization only, in which the entire bandwidth is normally used for the synchronization signal, has the advantage of being robust without affecting voice quality. A slight delay occurs at the beginning of a transmission while synchronization takes place, however. In some systems, part of a word can be missed at the receiver if the person transmitting begins speaking the instant he or she engages the PTT switch. In other systems, a slight delay is built in so that no part of the message is lost, but reception of the entire message is delayed by a fraction of a second from when it was spoken. This is usually not a problem, however, and will not even be noticed by those using systems which already include transmission path delays.

To achieve the best of both methods, robust initial synchronization can be combined with a less robust (and also with less effect on voice quality) continuous synchronization. The continuous sync portion permits late entry and clear voice override. Any lack of robustness in the synchronization, however, even that following the initial synchronization, should be compensated by higher safety margins in the design of the entire system, i.e., more repeaters, voting receivers, etc. Loss of communication, even for part of one transmission, could be fatal in law enforcement work.

4.4 Keys

All but the most simple voice privacy systems use a key that determines the rearrangement of the scrambled message. The key may be one of the inputs to an encryption algorithm which subsequently does the rearranging based on (1) the key, (2) the plain text input, and, in some cases, (3) the preceding section of cipher text. Or the key may be mixed with a "time of day" signal to provide initialization of a pseudo-random number generator which determines the rearrangement. In either case, it is absolutely essential that the key be kept secret,[12] that it contain a large number of characters (so that the number of combinations is too large for even the most sophisticated opponent to determine the key by computer driven trial and error methods), and also that the key be changed regularly. The latter is desirable to further reduce the possibility of the key being discovered, and also to reduce the number of messages that could be descrambled in the unlikely event that it is discovered. An opponent is not going to let you know when your key has been

[12]There are double key systems in use for the protection of data transmissions that allow one of the keys to be public knowledge. It is possible that such a system may someday be introduced into a voice privacy system.

discovered, so periodic changing of that key is good insurance. Keys and key management are thus important areas of concern for purchasers of voice privacy systems.

Questions pertaining to key management include: (1) how are the keys generated, (2) how are the keys distributed and changed, (3) how do those responsible keep track of the keys, and (4) what happens to the key when power is removed from the radio, e.g., to replace a battery nearing the end of its life. Obviously, the fewer people that know the key, the better will be the security. Knowledge of the particular key in use is not necessary to operate and use a scrambled voice transceiver.

Keys should be generated randomly. Any other method is likely to provide some useful information to a sophisticated opponent. The method for distribution and/or changing keys should be more advanced than simply asking each operator to punch in the correct key on his or her radio. There are several disadvantages to this method, among them being the time involved, the chance for error, especially when using long keys, and the fact that too many individuals know the key — some of whom might be susceptible to giving the information to the wrong people. Even if only one or two people are assigned the task of punching in the keys, the time involved is excessive and the chance for errors remains.

To circumvent the problems mentioned above, most voice privacy systems use a device known as a "key loader." One or more keys can be programmed into this device and subsequently downloaded automatically by connecting the key loader to each of the scrambled voice transceivers in the system. Knowledge of the specific keys used is not required by the person doing the downloading. In the best systems, the key loader operator receives some type of verification that the key has been correctly loaded. There is also some type of "lock" on the key loader so that the keys cannot be transferred except by authorized personnel.

Systems that permit the storage of more than one key are desirable both for increased security and for situations where different groups in the same agency may find it necessary to operate with separate keys. For example, keys "A" and "B" may be loaded into one group of radios, while keys "A" and "C" are loaded into another group. The two groups can communicate with each other using key "A," but each also has a key to keep conversations private to the group.

For systems that allow more than one key to be loaded into each transceiver, changing transceiver keys can be as simple as throwing a switch. In more sophisticated systems, an identifier could be included at the start of each message (or even during the message if continuous synchronization is used) to signify which of several stored keys is to be used to scramble and unscramble that particular message or portion of a message.

Some of the more advanced systems allow over-the-air rekeying (OTAR) of radios from a central location. The OTAR system may also include use of a wire line, e.g., phone line, for transceivers that are out of transmission range of the key sending location. The key to

be sent is encrypted by another key (a "key encryption key") which has previously been loaded into each of the radios in the system. When the new key is decoded and loaded properly, an acknowledgment is sent back to the sending location. Some systems also allow over-the-air elimination of the key, so that in the event a radio is lost or stolen, the operator at the central location can prevent that radio from being used for eavesdropping on scrambled communications.

Key storage within a radio should be designed so that it is impossible to determine the key (or the nonpublic contents of the encryption algorithm itself) by merely obtaining a radio and opening it up. The system should also be designed to prevent the unauthorized and undetected insertion, deletion or modification of the key. There should also be some means to detect errors in the operation of the encryption algorithm that could compromise the security of the system.

In many systems, the key is lost after a specific period of time following removal of the radio battery. An advantage to this is that radios left unattended in storage do not become a potential avenue for determining the key. A disadvantage is that the key can be lost if the operator spends too much time replacing a battery nearing the end of its life (thereby cutting this radio out of the secured communications system until it can be rekeyed). A few voice privacy systems allow the law enforcement agency to program what level of security it desires regarding key loss and key retention.

5. PURCHASING CONSIDERATIONS

5.1 General

Purchasing a voice privacy system presents problems that are different from those encountered when purchasing other types of communications equipment. Generally accepted standards exist for transmitters, receivers, antennas, etc., standards which define the parameters to be measured, the techniques for measurement and minimum performance requirements. Relationships between such parameters and communication range and intelligibility are well established. Such standards do not yet exist for voice privacy systems — one reason being that it is not yet possible to establish one set of relationships that is sufficiently accurate for all voice privacy systems. The information presented earlier can be used to make general predictions on the effect that a specific voice privacy system will have on characteristics of the communications system, but actual tests, with the voice privacy system installed, should be performed before the system is accepted.

Another reason that generally accepted standards do not yet exist for voice privacy systems is that security, which is the sole purpose of adding voice privacy to a communications system, is both difficult to specify and difficult to measure. Part of this problem is that the level of security depends, in part, on the level of attack. Some general information was presented in Section 4 that provides guidelines as to the amount of security

offered by a general class of systems against different levels of attack, but individual manufacturers may add proprietary embellishments to substantially increase security above the norm for a specific type of system.

Because of the lack of generally accepted standards for voice privacy systems, developing a set of specifications and putting them out for bid will probably not achieve the desired objective. An alternative is to negotiate with several suppliers before writing a firm contract. Instead of listing specific parameter values to be met, general objectives should be outlined, special needs identified, and a complete description of the communications system within which the voice privacy system will operate should be included along with other relevant facts. This general outline of requirements should then be sent to prospective suppliers and a request made that they submit a proposal identifying which of these requirements they can satisfy completely, partially, or not at all. The user should then evaluate the various proposals, contact those suppliers that most nearly meet the stated requirements and begin negotiations towards a final contract.

5.2 Types of Vendors and Systems

At the time this report was prepared, digital voice privacy was available only as part of a complete communications system. The vendor supplies radios with encryption and decryption modules installed, plus all the repeaters, base stations, control consoles, etc. that are required. The same vendor may also offer a system to which digital voice privacy can be added at some future time. This will be a system which is capable of digital transmission. The addition of encrypted voice will require that encryption and decryption modules be added to radios already designed to accept them, and possibly, that some minor modification be made to one or two other portions of the system. Often this modification can be as simple as replacing one modular rack or drawer in a console with another. As noted in Section 4.2, different digital encryption systems, even those from the same manufacturer, are not necessarily interoperable. This situation may change as progress is made toward a narrowband digital transmission standard.

Analog voice privacy is available most often in the form of an addition to either new or existing radios that transmit an analog signal. A scrambler/descrambler module is simply added to the radios. Sometimes, no modification to the communication system backbone is necessary. Vendors of the analog scrambling modules generally do not manufacture complete radios. A radio manufacturer that offers analog scrambling most often obtains the scrambling/descrambling module from one of the vendors listed in Section 5.3.

Several options exist for purchasing analog voice privacy: (1) new radios with analog voice privacy installed can be purchased from certain radio manufacturers (see table 1), or

(2) analog voice privacy can be added to either new or existing radios[13] by purchasing the scrambler/descrambler module (or modules) separately and having it installed in the radio. The user usually has four choices as to who does the installation: (1) a local distributor or radio shop (normally for new radios only), (2) the module vendor, (3) the user himself (if he has the capability), usually with guidance provided by the module vendor, or (4) an independent organization, such as a support and maintenance group, hired by the user.

The scrambling modules are now sufficiently small that they can, in most cases, be added inside the radio. Except for more complex systems, the days of an external attachment to the radio are gone. Because the modules are added inside, however, the process can be somewhat more complicated. Radio manufacturers often cooperate with the module vendor to make installation in certain radios relatively easy.

5.3 Vendor List

Except as noted, all the vendors listed in tables 1 and 2 provide a voice privacy system which is applicable to portable hand-held transceivers, in addition to the usual base stations and mobile units for vehicles and aircraft.[14] The radio manufacturers are listed separately from the module manufacturers. As noted in the previous section, the radio manufacturers that offer analog voice privacy systems usually obtain the necessary circuitry from one of the module vendors. Table 1 shows the type of voice privacy offered by each manufacturer plus the system name, if applicable. Table 2 gives the complete address for each manufacturer and the person or group to contact for additional information.

6. EVALUATION

An estimate of the security level offered by the prospective voice privacy system should be made *early* in the procurement process. If the level of security, i.e., voice privacy, is not adequate, the systems' effect on other parameters is irrelevant. Before acceptance, the voice privacy system should also be evaluated for range, intelligibility and speaker recognition in both the clear and coded modes of operation. An initial evaluation of these parameters early in the procurement process is desirable but should not substitute for a final evaluation after everything is in place.

---

[13]Analog voice privacy can be added to many makes of radio. Contact a local distributor or radio shop for information or contact the module vendors themselves for information as to which radios they can modify.

[14]The vendors listed comprise all that were identified at the time this report was prepared. Their presence in the tables does not represent an endorsement by either the U.S. Department of Justice, or the National Institute of Standards and Technology.

Table 1. Type of voice privacy offered by each vendor.

Vendors	Type of Voice Privacy Offered					
	Digital (see section 4.2 description)		Analog (see section 4.1 for description)			
Radio Manufacturers	All digital	Clear voice analog/ Protected voice digital	Bandsplitters	Split-band inversion	Frequency-hopping inversion (see note 1)	Fixed or simple inversion
Bendix/King Lawrence, KS		X E-Series DES				X
Comm-Tech International Orlando, FL					X Kryptic Radio	
Cycomm Corp. Portland, OR			See note 2			
Ericsson GE Lynchburg, VA	X Aegis	X Voice Guard				
Icom Bellevue, WA					X	
Midland Radio Kansas City, MO				X	X	X
Motorola, Inc. Schaumburg, IL	X Astro	X Securenet; Advanced Securenet				
Module Manufacturers						
Midian Electronics, Inc. Tucson, Arizona				X	X	X
MX-Com, Inc. Winston-Salem, NC				X		X
Pacific Circuit Design Sidney, BC, Canada				X		
Selectone Corp. Hayward, CA					X	X
Technical Communications Corp. Concord, MA		See note 3 DSP 9000 HS	X DSP 280			
Transcrypt International, Inc. Lincoln, NE					X	X

Note 1: Also known as "rolling" code scramblers.

Note 2: This manufacturer produces a time division multiplex system (see sec. 4.1.2) but at the time this report was prepared, the system was not applicable to hand-held portable radios.

Note 3: The module is contained in a separate handset to be used in conjunction with a backpack portable radio. The audio is converted to digital for scrambling but converted back to analog for transmission over narrow band channels. Designed originally for tactical military use, it can also be used by law enforcement agencies whose high security needs justify the added expense.

Table 2. Vendor addresses.

Radio Manufacturers

Bendix/King
Mobile Communications Division
2920 Haskell Avenue
Lawrence, Kansas 66046-0347

Sales Department (913) 842-0402
(800) 648-0947

Comm-Tech International, Inc.
5401 Alhambra Drive, Suite B
Orlando, Florida 32808-7081

Evelyn Stone (407) 291-9009

Cycomm Corporation
6665 SW. Hampton
Portland, Oregon 97223

Phil Bailey (503) 620-1024
(800) 523-8636

Ericsson G.E. Mobile Communications Inc.
Mountain View Road
Lynchburg, Virginia 24502

Bob Nunley (804) 528-7630
Telesales (800) 541-3840

Icom America, Inc.
2380-116th Ave. NE.
Bellevue, Washington 98004

Sandy Williams (206) 454-8155

Midland Radio
1690 North Topping Ave.
Kansas City, Missouri 64120

Telemarketing (816) 241-8500
(800) 643-5263

Motorola Inc.
1301 E. Algonquin Road
Schaumburg, Illinois 60196

(708) 576-9049

Module Manufacturers

Midian Electronics, Inc.
2302 East 22nd Street
Tucson, Arizona 85713

Bob Serensca (602) 884-7981
(800) 643-4267

MX-Com, Inc.
4800 Bethania Station Road
Winston-Salem, North Carolina 27105-1201

Doug Thomson (919) 744-5050
(800) 638-5577

Pacific Circuit Design
P.O. Box 2610
#8-10114 McDonald Park Road
Sidney, British Columbia, Canada V8L 4C1

Paul Fox (604) 656-8849

Transcrypt International, Ltd.
1620 North 20th Street
Lincoln, Nebraska 68503

Sales Department (402) 435-4400
(800) 228-0226

Selectone Corporation
23278 Bernhardt Street
Hayward, California 94545-1621

Patrick O'Rourke (510) 887-1950
(800) 227-0376

Technical Communications Corporation
100 Domino Drive
Concord, Massachusetts 01742

Dale Peterson (617) 862-6035

Voice privacy can be checked at its most elementary level by having several persons simply listen repeatedly to a coded communication, e.g., a recording of the message played over and over, to see if any of them can eventually decipher the content. The human brain is very adaptable. Some people, with a combination of careful listening and intelligent guesswork might eventually learn to understand most of a message that is coded by one of the simpler systems. Decoding beyond this level usually requires the use of additional electronic equipment and the knowledge of cryptoanalytic techniques. Success depends to a large extent on the abilities of the opponent and the amount of equipment he can afford to mount his attack. There is also the time element to consider. Even if scrambled speech can eventually be descrambled, it may be too late to do the opponent any good.

There are no universally accepted methods to determine the security offered by a specific system. Some information was presented in Section 4 that provides general guidelines as to the amount of security offered by different types of voice privacy systems against different levels of attack. It must be remembered, however, that individual manufacturers may add proprietary embellishments to substantially increase security above the norm for a specific type of system.

The evaluation of communications range, intelligibility and speaker recognition must be done in a way that reduces or eliminates the variabilities introduced by a particular speaker, listener, message content, transmission path and/or set of environmental conditions. The usual method is to use enough speakers and listeners to average out individual differences and to use a set of standard words, numbers, phrases, etc. recorded by each speaker for reception by each listener.

Intelligibility and speaker recognition tests should be done in both the laboratory and in the field. Laboratory conditions are easier to control and are useful for changing environmental conditions, but field tests may offer a more realistic assessment. A comparison should be made between the clear voice signal of both the present system and the new system and the descrambled voice signal of the new system. Range must be evaluated in the field. The evaluation can be done by continually increasing the distance between transmitter and receiver until a certain percentage of the previously recorded set of words, numbers and phrases can no longer be understood. First compare the clear mode of the new system with the clear mode of the present system, and then switch back and forth between the clear and scrambled modes of the new system. The evaluation should be done in more than one area to eliminate variations due to the terrain.

Ideally, range, intelligibility, and speaker recognition should also be checked under the extremes of environmental conditions that are likely to be faced in the field. Depending on the time of year, however, at least one extreme may be difficult to simulate in the field. Results from the laboratory tests can be used instead.

7. REFERENCES

[1] Beker, Henry J. and Piper, Fred C. Secure speech communications. Chapter 4 on Frequency domain scrambling, Section 4 on Band splitters. Orlando, Florida: Academic Press, Inc; 1985, pp. 138-149.

[2] National Communications System. Telecommunications: Analog to digital conversion of radio voice by 4800 bit/second code excited linear prediction (CELP). Federal Standard 1016. Washington DC; National Communications System (NCS), Office of Technology and Standards, February 14, 1991.

[3] National Institute of Standards and Technology. DES modes of operation. Federal Information Processing Standards (FIPS) Publication 81. Washington, DC: U.S. Department of Commerce, National Institute of Standards and Technology (NIST), December 2, 1980.

[4] National Institute of Standards and Technology. General security requirements for equipment using the data encryption standard. Federal Information Processing Standards (FIPS) Publication 140 (formerly Federal Standard 1027). Washington, DC: U.S. Department of Commerce, National Institute of Standards and Technology (NIST), April 14, 1982.

8. BIBLIOGRAPHY

Beker, Henry J. and Piper, Fred C. Secure speech communications. Orlando, Florida: Academic Press, Inc; 1985.

Bishop, Don. How analog scrambling fits tactical security needs. Mobile Radio Technology, Vol. 8, No. 7, pp. 48-50, July 1990.

Carmody, Jack. Primer: Ways to turn voice signals into digital codes. Data Communications, Vol. 13, No. 11, pp. 108-113, October 1984.

Crandall, Gordon A. III. Assessment of digital radio voice protection for government land-mobile use. NTIA Technical Memorandum 87-122. Washington, DC: U.S. Department of Commerce, National Telecommunications and Information Administration; July 1987.

Dennis, George. In bits and pieces. Communications, Vol. 22, No. 10, pp. 44-48, September 1985.

Inglis, Andrew F., ed. Electronic Communications Handbook. Chapter 11 on signal transmission modes, section on spread-spectrum modulation techniques. New York: McGraw-Hill Book Company; 1988. pp. 11.20 to 11.25.

Jayant, N. S. Coding speech at low bit rates. IEEE Spectrum, Vol. 23, No. 8, pp. 58-63, August 1986.

Kelley, S. and Wallace, H. Split-band scrambing furnishes voice security. Mobile Radio Technology, Vol. 6, No. 5, pp. 18-28, May 1988.

McKernan, E. J. and Scott, B. A rolling code scrambler gathers diverse functions. Mobile Radio Technology, Vol. 7, No. 7, pp. 42-58, July 1989.

National Institute of Standards and Technology. Data encryption standard. Federal Information Processing Standards (FIPS) Publication 46-1. Washington, DC: U.S. Department of Commerce, National Institute of Standards and Technology (NIST), January 22, 1988.

Nelson, Robert E. A guide to voice scramblers for law enforcement agencies. NBS Special Publication 480-8. Washington DC: U.S. Department of Commerce, National Institute of Standards and Technology, 1976.

Nye, J. Michael. Who, what and where in communications security. Hagerstown, MD: Marketing Consultants International, Inc.; 1981, 1986.

Speights, William D. Assessment of digital radio voice protection for government land-mobile use. NTIA Technical Memorandum 88-137. Washington, DC: U.S. Department of Commerce. National Telecommunications and Information Administration, September 1988.